CLAIMS

1. A method of uniforming physical random numbers, comprising the steps of: inputting a plurality of physical random numbers to a random number holding device (200) to hold them, employing a part of physical random numbers held in said random number holding device as an address of a selector, and randomly selecting and outputting physical random numbers from the residual part, based on said address.

2. A method of uniforming physical random numbers according to claim 1, comprising the steps of: randomly selecting the random numbers held in said random number holding device, employing a logical product circuit, instead of said selector, and outputting an exclusive OR of them.

3. The method of uniforming physical random numbers according to claim 1, wherein an exclusive OR circuit that inputs the output of said selector and the physical random number is provided, its output being input into the random number holding device (200).

4. A method of uniforming physical random numbers, comprising uniforming physical random numbers at multiple stages by repeating the operation according to any of claims 1 to 3 two or more cycles.

5. The method of uniforming physical random numbers according to any one of claims 1 to 4, wherein a shift register (200) is employed as the random number holding device.

6. A physical random number generation device having a physical random number generator, said physical random number generator comprising:

a serial physical random number generator for generating a serial random number in accordance with a reference clock signal;

a serial/parallel converter for converting the serial random number to a parallel random number;

a plurality of registers capable of holding the parallel random number; and

a control circuit for sequentially holding the parallel random number in said registers every time the parallel random number is generated by said serial/parallel converter, and reading and outputting the parallel random number from said register in accordance with a read clock signal, as well as successively updating the contents of said registers by shifting the parallel random number from the other register to the register for which the reading is ended.

7. The physical random number generation device according to claim 4, wherein said physical random number generator comprises an up/down counter for deciding a register to hold the parallel random number among the plurality of registers

and outputting a write address, a selector for selecting the register to hold the parallel random number, based on the write address output by said up/down counter, to output a load signal, and a control circuit for sequentially holding the parallel random numbers in said serial/parallel converter from the latter stage register to the former stage register among said registers, based on the load signal from said selector, and reading and outputting the parallel random number from said last stage register among said registers in accordance with a read clock signal, as well as sequentially shifting the parallel random number within each register residing at the former stage of said register to the latter stage.

8. The physical random number generation device according to claim 6 or 7, wherein said physical random number generator comprises a total counter for counting the total number of serial random numbers generated by said serial physical random number generator, and a random number verification circuit for verifying the uniformity of random numbers, based on the serial random numbers, when the total number of serial random numbers counted by said total counter reaches a predetermined bit number.

9. The physical random number generation device according to claim 8, wherein a random number verification method for said random number verification circuit comprises verifying the uniformity of random numbers by counting the appearance

frequency of a random number value "0" or "1" and comparing it with a prescribed value.

10. The physical random number generation device according to claim 8, wherein a random number verification method for said random number verification circuit comprises verifying the uniformity of random numbers by comparing a χ square value calculated based on the appearance frequency of each random number value with a prescribed value, with one random number value being 4 bits.

11. The physical random number generation device according to claim 8, wherein the random number verification method for said random number verification circuit comprises verifying the uniformity of random numbers by counting the appearance frequency of string for every length of string and comparing it with a prescribed value.

12. The physical random number generation device according to claim 8, wherein the random number verification method for said random number verification circuit comprises verifying the uniformity of random numbers by comparing the length of the longest string appearing in the random numbers of certain bits with a prescribed value.

13. The physical random number generation device according to any one of claims 6 to 12, further comprising the chip select

and output enable functions and the corresponding terminals, in which a buffer function of an output section has three states.

14. The physical random number generation device according to any one of claims 6 to 13, further comprising a plurality of physical random number generators, in which one physical random number generator is selected from among said physical random number generators, based on a select signal of said selector, to output the random number or random number verification data.

15. A physical random number generator comprising:

two integration circuits for integrating a clock signal through a resistor and a capacitor to output an integral waveform, two noise sources, two amplifiers for amplifying the noise of said noise source to output a noise signal, two mixers for mixing said integral waveform and said noise signal, and two edge detection circuits for detecting the first edge of jitter generated based on an output waveform of said mixer;

a flip-flop for outputting "0" or "1" based on a phase difference in the output signal between said edge detection circuits;

a phase adjuster for adjusting the phase of an input signal input into said each integration circuit, said phase adjuster having a delay, a first selector and an up/down counter; and

a feedback circuit for feeding back the output of said flip-flop to said phase adjuster so that "0" or "1" output from said flip-flop may converge to 50%;

wherein a second selector and a third selector are provided at the former stage of said each integration circuit, and

a polarity switching circuit is provided for switching the polarity of input for said first selector, said second selector and said third selector by the most significant bit of said up/down counter.

16. A physical random number generator comprising:

one integration circuit for integrating a clock signal through a resistor and a capacitor to output an integral waveform, two noise sources, two amplifiers for amplifying the noise of said noise source to output a noise signal, two mixers for mixing said integral waveform and said noise signal, and two edge detection circuits for detecting the first edge of jitter generated based on an output waveform of said mixer; and

a flip-flop for outputting "0" or "1" based on a phase difference in the output signal between said edge detection circuits;

wherein a variable delay composed of a delay and a selector to adjust the phase of an input signal input into said flip-flop is provided at the former or latter stage of said each edge detection circuit, and a feedback circuit for feeding back

the output of said flip-flop to said variable delay so that "0" or "1" output from said flip-flop may converge to 50%.

17. The physical random number generator according to claim 15 or 16, wherein an FET (Field Effect Transistor) is additionally provided in parallel to the capacitor of said integration circuit at the latter stage of the resistor of said integration circuit.

18. The physical random number generator according to any one of claims 15 to 17, wherein a constant current circuit is provided instead of the resistor in said integration circuit.

19. A physical random number generation device wherein two or more physical random number generators according to any one of claims 15 to 18 are connected in parallel, and the parallel physical random numbers input into said each physical random number generator are rearranged into the serial physical random numbers that are then output.